Chapter 3

First Response

Planning and Preparation - 1

- The Who, What, When, Where and How
  - Physical Location
    - Type of location – residence, business, apartment building
    - Size – Internet access, office or floor or whole business, multiple buildings, neighborhood
  - Personnel
    - Know who will be present during your incident-response planning
    - Will you be working at a business during business hours with workers present
      - Get to know personnel – can you find a "friendly" administrator you know is not involved
    - Is the suspect known
      - Find out as much about them as possible
        - Where they work, username, email, home address, car, photo, etc.

Planning and Preparation - 2

- The Who, What, When, Where and How
  - Computer Systems
    - What OS, type of computer
    - Encryption – indication
    - Network – wireless, wired etc, servers, backups, proxy, firewalls
    - What type of evidence – child pornography, bootleg software, “booked books”
    - Admin. Password – who has them, admin helpful or part of the problem
    - Seized or on location – in a lab or within a limited amount of time
    - What your authority is - searching
- What to take with you
  - Digital camera, cables, cords, floppy, usb, Forensic boot, gloves, image RAM, portable field computer/laptop, adapters, labels, bags, hubs, PC reference guide, etc.

Planning and Preparation - 3

- Search Authority
  - Search Warrant
    - Consent to search
  - Call from victim
  - Corporate counsel
    - Policy
    - Court order for civil suit
- WE are BOUND by the SEARCH AUTHORITY
  - All 1st responders need to be aware of the limits
    - Specific computers, file types, user files etc.
    - Must stay within the boundaries
    - Contingency plan for evidence that might be discovered in plain sight exceeding the search authority
    - Usually you must leave behind a list of what was taken and the warrant

Handling Evidence at the Scene - 1

- Securing the Scene
  - Safety #1 priority
  - Perimeter control - secure area and provide ongoing security
- Recording and Photographing the Scene
  - How things are found when you enter the scene
    - Recorder – takes detailed notes of everything seized
    - Photographer – Photographs or videos area
    - Search-and-Seizure specialist – seizes and bags and tags non-digital evidence
    - Digital evidence search-and-Seizure specialist – seizes, bags and tags digital evidence

Handling Evidence at the Scene - 2

- Considerations for Seizing Computer Evidence
  - Physical Evidence
    - Fingerprints, hairs, fibers etc.
    - Coordinate your efforts with other examiners
    - Bare minimum – use latex gloves as a standard practice
    - Tyvek suit if other fibers or bodily tissue might be examined
    - PROTECT EVIDENCE – digital and physical

Handling Evidence at the Scene - 3

- Volatile Digital Evidence
  - Turn your attention to capturing digital evidence
    - RAM – current state might be a necessity for your investigation
      - EnCase – Snapshot
        - Analysis and imaging of live systems
      - Utilize tools such as CryptHunter to see if encryption is enabled
      - If you don't have a live capture option you must use command line tools
        - Should research and try before you complete any investigations with these tools

Handling Evidence at the Scene - 4

- Shutdown Procedures
  - Chart on page 107
  - Dictated by OS
    - OS – usually pull the plug
      - WIN Flavors up to 7
      - Linux/Unix
      - Mac
    - Servers – proper shutdown
    - Might be other reasons to do something different
- Bagging and Tagging
  - Chain of Custody
  - Proper handling to lab

DOL Disclaimer and CCBY

This workforce product was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The product was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Except where otherwise noted, this work by Central Maine Community College is licensed under the Creative Commons Attribution 4.0 International License.